IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA,	)	
	)	
v.	)	**Criminal Action No. 1:20-cr-143**
	)	**UNDER SEAL**
ZACKARY ELLIS SANDERS,	)	
Defendant.	)	

SEALED MEMORANDUM OPINION

At issue in this production, possession, and receipt of child pornography prosecution is whether the Magistrate Judge had probable cause to issue a search warrant for Defendant Zackary Ellis Sanders' residence and whether Federal Bureau of Investigations ("FBI") Special Agent Christopher Ford intentionally or recklessly materially misled the Magistrate Judge in his affidavit in support of a warrant. For the reasons that follow,

> (i) the Magistrate Judge had an adequate and substantial basis for finding probable cause to issue the search warrant,
>
> (ii) the Affidavit contains no material misrepresentations or omissions, and
>
> (iii) defendant failed to make the requisite substantial preliminary showing that Special Agent Ford made a material false statement knowingly and intentionally, or with reckless disregard for the truth.

Therefore, defendant's Motions to Suppress must be denied.

I.

The following facts are derived from the record in this case and are relevant to the resolution of defendant's Motions to Suppress.

- On August 19, 2019, the Federal Bureau of Investigation ("FBI") received a tip from a reliable foreign law enforcement agency ("FLA") [redacted] that:

> On 2019-05-23 02:06:48 UTC [the Target IP address] was used to access online child sexual abuse and exploitation material, with an explicit focus on the facilitation of sharing child abuse material (images, links and videos) [redacted]. Users were required to create an account (username and password) in order to access the majority of the material.

FLA August 19, 2019 [redacted] Report, Def. Ex. 1, Dkt. 86, ("FLA Tip").

- On September 10, 2019, the FBI issued an administrative subpoena to Cox Communications for information relating to the Target IP address. January 17, 2020 FBI Report Opening Investigation, Form FD-1057, Def. Ex. 4, at 2, Dkt. 86 ("FD-1057"). Cox Communications identified the subscriber, Risa Sanders, and Target Residence in McLean, Virginia. *Id.*

- On September 16, 2019, the FLA sent a letter to a Supervisory Special Agent at the FBI stating that the FLA had provided the FBI with "data . . . in relation to internet addresses (IPs), associated to individuals who have accessed online Child Sexual Abuse and Exploitation material." FLA September 16, 2019 Letter, Def. Ex. 2, Dkt. 86, ("FLA Letter"). The FLA Letter states that the IP address data was "obtained [redacted]" based on two warrants [redacted]. *Id.* The FLA Letter further states that "at no time was any computer or device interfered with in the United States" and that "during an independent investigation lawfully authorized under [redacted] legislation, the [redacted] did not access, search or seize any data from any computer in the United States." *Id.*

- On October 25, 2019,[1] the FLA provided to the FBI an [redacted] Report for an operation [redacted] stating that "[t]his site had an explicit focus on the facilitation of sharing child abuse material." FLA October 25, 2019 [redacted] Report, Def. Ex. 3, Dkt. 86, ("FLA [redacted] Report").[2]

- On January 17, 2020, Special Agent Christopher Ford wrote a report to open an investigation into the Target IP address. FD-1057. Special Agent Ford's report describes a website [redacted] as "an online bulletin board dedicated to the advertisement and distribution of child pornography that operated from approximately 2016 to June 2019." *Id.* at 1.

---

[1] The government represents that the FLA [redacted] Report was sent from the FLA to the FBI on October 25, 2019. The document itself lists the "Time/Date of Report" as "27/07/2020 15:59," but counsel for the government explains that this document's listed date was the product of an automatic update performed by Microsoft Word, not a reflection of when the document was transmitted.

[2] The FLA [redacted] Report also identifies five images or videos shared on the [redacted] website and states that "[t]his site had an explicit focus on the facilitation of sharing child abuse material (images, links and videos) [redacted]. Users were required to create an account (username and password) in order to access the majority of the material." FLA [redacted] Report. The FLA [redacted] Report *does not* state that the Target IP address created or accessed the five images or videos identified in the Report.

- Special Agent Ford's report states that "[i]n August 2019, the FBI received information from a foreign law enforcement agency (FLA) known to the FBI with a history of providing reliable, accurate information in the past that [the] FLA identified a user who accessed [redacted] using [the Target IP address] on May 23, 2019, at 02:06:48 UTC." *Id.* at 2.

- Special Agent Ford's report reflects that the FBI obtained information about the IP address subscriber, Risa Sanders, and the other residents at the Target Residence, Jay H. Sanders and Zackary E. Sanders. FD-1057 at 3. The report identifies Risa Sanders as a licensed clinical psychologist. *Id.*

- Special Agent Ford's report concludes that "[b]ased on the provided information, the user of the [Target IP address] is in violation of 18 U.S.C. 2252(a)(2) Sexual Exploitation of Children, specifically distribution of child pornography." FD-1057 at 4.

- On February 10, 2020, Special Agent Ford applied for a search warrant and submitted an affidavit in support of the application. In the Affidavit, Special Agent Ford averred:

> A user of the internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography via a hidden service website that operated on the Tor anonymity network. The website is described below and referred to herein as the "TARGET WEBSITE." There is probable cause to believe that a user of the internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE, as further described herein.

Special Agent Ford Affidavit, Def. Ex. 5, at ¶ 6, Dkt. 86 ("Affidavit").[3]

- Special Agent Ford also averred that:

> In August 2019, a foreign law enforcement agency ("FLA") known to the FBI and with a history of providing reliable, accurate information in the past, notified the FBI that the FLA determined that on May 23, 2019, a user of the [Target IP address] accessed online child sexual abuse and exploitation material via a website that the FLA named and described as the TARGET WEBSITE.

Affidavit ¶ 23.

- Special Agent Ford further averred that:

> The FLA described the website as having "an explicit focus on the facilitation of sharing child abuse material (images, links and videos), [redacted]

[3] The Tor network, or "The Onion Router" network, is a network that allows users to anonymously access the internet. To access the Tor network, users must either download the Tor browser or manually configure their web browser.

> [redacted] stated that "[u]sers were required to create an account (username and password) in order to access the majority of the material," and provided further documentation naming the website as the TARGET WEBSITE, which the FLA referred to by its actual name.

Affidavit ¶ 24.

- Special Agent Ford also averred that:

> The FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of U.S. law enforcement sharing criminal investigative information with the FLA and the FLA sharing criminal investigative information with U.S. law enforcement, across disciplines and including the investigation of crimes against children. The FLA advised U.S. law enforcement that it obtained that information through independent investigation that was lawfully authorized in the FLA's country pursuant to its national laws. The FLA further advised U.S. law enforcement that the FLA had not interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain that IP address information. U.S. law enforcement personnel did not participate in the investigative work through which the FLA identified the IP address information provided by the FLA.

Affidavit ¶ 25.

- On February 10, 2020, Magistrate Judge John F. Anderson authorized the search warrant for defendant's residence. Two days later, on February 12, 2020, law enforcement agents executed the search warrant.

- During the search of defendant's residence, law enforcement agents uncovered evidence of production, receipt, and possession of child pornography. Evidence included an interview with defendant in which the defendant admitted to accessing and receiving child pornography through websites on the Tor network, including the [redacted] website, as well as an Apple iPad with numerous conversations on it between defendant and purported minors in which defendant persuaded and attempted to persuade purported minors to produce images and videos of themselves engaging in sexually explicit conduct and to send those images and videos to defendant, and a laptop with multiple videos and images depicting minors engaged in sexually explicit conduct. Affidavit in Supp. of a Crim. Compl. and an Arrest Warrant, at 5, 12, Dkt. 4.

Based on the evidence presented to the grand jury, a twelve-count indictment was returned on June 24, 2020, charging defendant with:

> (i) five counts of production of child pornography, in violation of 18 U.S.C. § 2251(a) and § 2251(e),

(ii) six counts of receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and § 2252(b)(1), and

(iii) one count of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B) and § 2252(b)(2).

Indictment, at 2-4, Dkt. 29.

On July 13, 2020, defendant filed a Motion to Compel Discovery related to alleged misrepresentations in Paragraphs 23 and 25 of the Affidavit. After briefing and oral argument, an Order issued on August 21, 2020, denying defendant's Motion to Compel. *United States v. Sanders*, No. 1:20-cr-143 (E.D. Va. Aug. 21, 2020) (Order Denying Def. Mot. to Compel).

On September 2, 2020, defendant filed four Motions to Suppress and a Renewed Motion to Compel or in the Alternative for Reconsideration of the Court's Order Denying his Motion to Compel. On September 10, 2020, an Order issued denying defendant's Motion to Reconsider the August 21, 2020 Order. *United States v. Sanders*, No. 1:20-cr-143 (E.D. Va. Sept. 10, 2020) (Order Denying Def. Mot. to Recons. (Sealed)). On September 11, 2020, a hearing was held on defendant's Motions to Suppress. This matter has been fully briefed and orally argued and is now ripe for disposition. For the reasons that follow, defendant's Motions to Suppress must be denied.

II.

Defendant argues that the search of his home violated the Fourth Amendment because it was not supported by probable cause. This argument is meritless; the record evidence makes clear that the Magistrate Judge had a substantial basis for concluding that someone at the target residence had accessed or had attempted to access child sexual abuse and exploitation material and that probable cause existed to issue the search warrant.

Probable cause for a search warrant exists when, "given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). It is "therefore 'not a high bar.'" *United States v. Bosyk*, 933 F.3d 319, 325 (4th Cir. 2019) (quoting *D.C. v. Wesby*, 138 S. Ct. 577, 586 (2018)), *cert. denied*, 140 S. Ct. 1124 (2020). Thus, the Court "must accord 'great deference' to the magistrate's assessment of the facts." *United States v. Blackwood*, 913 F.2d 139, 142 (4th Cir. 1990). As the Supreme Court affirmed in *Illinois v. Gates*, a magistrate's determination of probable cause is proper so long as the magistrate has "a substantial basis for determining the existence of probable cause." *Gates*, 462 U.S. at 239 (1983).

In this case, the Magistrate Judge clearly had a substantial basis to conclude that, given the totality of the circumstances, there was a fair probability of finding evidence that the internet user at the Target IP Address accessed or attempted to access child sexual abuse and exploitation material. Special Agent Ford's Affidavit accurately reiterates the FLA's Tip that the internet user "accessed online child sexual abuse and exploitation material via a website that the FLA named and described [redacted]." Affidavit ¶ 23. The Affidavit also establishes that the [redacted] website was a Tor hidden service accessible only through the Tor network. *Id.* at ¶ 27.[4] Additionally, the Affidavit communicates that, as such, the website would be substantially more difficult to navigate to than an ordinary internet website. *Id.*[5] The Affidavit further outlines the "numerous affirmative steps" required by a user to access the [redacted] website and explains

[4] As a general matter, Tor hidden services operate in a manner designed to obscure the true IP address and location of the server hosting the website. These features of Tor hidden services hinder efforts to determine the true IP address and location of a server hosting Tor hidden services. Tor hidden services can only be accessed through the Tor browser or by manually configuring a web browser to access the Tor network. *See* Affidavit.

[5] The Affidavit explains that directory sites [redacted] and Tor hidden services generally, are similarly difficult to navigate to because they are comprised of a 16-or-56-character web address containing a largely random string of numbers and letters. Affidavit at ¶¶ 14, 27. The Affidavit further explains that Tor hidden services are much more difficult to find using a search engine because such sites are not indexed to the same extent as websites on the open internet. *Id.* at ¶ 27.

that it was thus "extremely unlikely that any user could simply stumble upon [the [redacted] website] without understanding its purpose and content." *Id.* at ¶ 29. Finally, the Affidavit reasonably concludes that there is at least a "fair probability that contraband or evidence of a crime" would be found at the target residence. *Gates*, 462 U.S. at 238; Affidavit ¶¶ 37-52.[6]

Given these facts, Fourth Circuit and persuasive precedent supports the Magistrate Judge's finding of probable cause to issue the search warrant in this case. Indeed, the Fourth Circuit and other courts have affirmed the finding of probable cause in cases with similar facts where the supporting affidavit provided essentially similar, or less, information. Especially instructive in this regard is *United States v. Bosyk*, 933 F.3d at 319. In *Bosyk*, the Fourth Circuit affirmed the issuance of a search warrant based on an affidavit that alleged only that Bosyk's IP address was used to access a page on a file-sharing website containing encrypted child pornography files, and that a link to that page had been posted on a Tor site with images of child pornography. *Bosyk*, 933 F.3d at 319. On those facts, the Fourth Circuit found that the Magistrate Judge had a substantial basis for determining probable cause because, "although the search relied on a 'single click' of an internet link, the click was to a video of child pornography in circumstances suggesting the person behind that click plausibly knew about and sought out that content." *Id.* at 326. Other circuits likewise have affirmed probable cause findings based only on one or two acts, and indeed notably courts have done so in cases that did not involve, as here, the significant added difficulty of accessing child pornography on a Tor hidden service [redacted]

[6] The Affidavit does so by describing characteristics common to individuals with a sexual interest in children or sexually explicit depictions of children. Thus, this portion of the Affidavit establishes that there was a fair probaility of finding evidence of a crime at the residence of the Target IP Address user despite the privacy features of the Tor browser discussed by the defendant that make evidence of the defendant's May 23, 2019 visit to the [redacted] website unlikely to be found in a the browser's cache or elsewhere on the computer. Taken together with the nature of Tor web addresses, these common characteristics make it so the Magistrate Judge had a substantial basis to conclude that there was a fair probability of finding evidence of a crime, such as bookmarks or lists of sites dedicated to child pornography or of directory sites dedicated to the same.

[redacted].[7] Here, the Affidavit not only establishes that the Target IP address accessed child sexual abuse and exploitation material on a Tor hidden service, but also explains the various steps an internet user has to go through in order to access the website. These facts provide an even more substantial basis for finding probable cause to issue the warrant than existed in *Bosyk*.

Seeking to avoid this result, the defendant first argues that the FLA Tip upon which the Affidavit relied was uncorroborated hearsay that could not support a finding of probable cause. This argument is unconvincing and contradicted by established precedent. As a general matter, the Supreme Court has made clear that "an affidavit relying on hearsay 'is not to be deemed insufficient on that score, so long as a substantial basis for crediting the hearsay is presented.'" *Gates*, 462 U.S. at 241–42 (citing *Jones v. United States,* 362 U.S. 257, 269 (1960)). In this case, there is more than a substantial basis for crediting the hearsay. As the Affidavit established, the FLA is a law enforcement agency that is well-known by the FBI and that has a long history of sharing reliable information with the United States. It is well-established that proven, reliable informants generally and law enforcement agencies in particular are entitled to considerable credence. *See United States v. Bynum*, 293 F.3d 192, 197 (4th Cir. 2002) ("[A] proven, reliable informant is entitled to far more credence than an unknown, anonymous tipster."); *United States v. Hodge*, 354 F.3d 305, n. 1 (4th Cir. 2004) (stating that law enforcement officers "'are plainly . . . reliable' even without any special showing" (quoting *United States v. Ventresca,* 380 U.S. 102, 111 (1965))).

Nor is there any doubt that this presumption of credibility extends to reliable foreign law enforcement agencies like the FLA in this case[redacted].

[7] *See United States v. Vosburgh*, 602 F.3d 512 (3d Cir. 2010) (affirming the finding of probable cause to issue a warrant based on an individual's attempted download of child pornography from a dedicated message board). *See also United States v. Contreras*, 905 F.3d 853, 858 (5th Cir. 2018) ("[O]ur court, as well as others across the country, has found probable cause to search a residence based on just one or two uploads of child pornography.").

The Third Circuit stated this presumption clearly in *United States v. Benoit* in its affirmance of the Coast Guard's reliance on a tip from Grenadian law enforcement authorities based on the fact that the agency was a known and a repeat player in a working relationship with the Coast Guard. *United States v. Benoit*, 730 F.3d 280, 285 (3d Cir. 2013) ("[A] tip from one federal law enforcement agency to another implies a degree of expertise and a shared purpose in stopping illegal activity, because the agency's identity is known."). Given this FLA's history of providing reliable tips to the FBI and this FLA's status as a respected foreign law enforcement agency, it was reasonable for the Magistrate Judge to rely on the FLA Tip without further corroboration by the FBI.

The defendant next argues that the FLA Tip was insufficient for the Magistrate Judge to infer that the Target IP Address user had viewed or downloaded child pornography or even intended to do so. This argument is also unconvincing; it relies on a wishful misreading of Paragraph 23 of the Affidavit. It ignores information provided in other portions of the Affidavit and conflates the standard for issuance of a search warrant—namely fair probability that contraband will be found at the location of the Target IP Address—with the standard for conviction of a crime—namely proof beyond a reasonable doubt. Paragraph 23 accurately reports the FLA Tip, stating that the Target IP Address "accessed online child sexual abuse and exploitation material." Affidavit ¶ 23. The Affidavit also describes the steps the Target IP Address user had to take to navigate through Tor and then to the [redacted] website and its offerings. Thus, the Target IP Address user's arrival at the [redacted] website was no mere happenstance; rather, the information in the Affidavit noting the steps the Target IP Address user was required to take to navigate to the Tor hidden service [redacted] warrants the inference that the Target IP Address user's arrival at the [redacted] website was purposeful, that is the Target IP

Address user's purpose was to access the website and its illegal content. It follows that the Magistrate Judge had a substantial and sound basis for concluding that there was a fair probability that child sexual abuse and exploitation material would be found at the Target IP Address user's residence.

Nor is the Magistrate Judge's conclusion negated by the length of time between defendant's accessing the [redacted] website and the issuance of the search warrant. As the Affidavit notes, there is a well-established tendency in individuals with a sexual interest in children to collect and retain child pornography. Affidavit ¶¶ 41-48. Indeed, the Fourth Circuit recognized this tendency in *Bosyk* when it noted that "individuals who possess or access with intent to view child pornography [tend] to collect such material and *hoard it for a long time*." *Bosyk*, 933 F.3d at 331 (internal quotation marks omitted) (emphasis added). In sum, the Affidavit provides more than ample reason to believe that evidence of the Target IP Address user's activity would be recoverable even eight months after the user allegedly accessed child sexual abuse and exploitation material on the [redacted] website.

Also unavailing to defendant is the claim that the [redacted] website included legal as well as illegal content. Defendant bases this argument solely on the website's mention of "18" and "hurtcore" content.[8] A thorough examination of screenshots of the [redacted] website provided by the FBI reveal defendant's claim to be baseless. *See* [redacted] Board Index, Def. Ex. 10, Dkt 86. The [redacted] website's board index is divided into categories for "Ages 0-5," "Ages 6-13," and "Ages 14+". *Id.* Even the subforum for "Regular Porn" has a subheading of "[t]eens and under." *Id.* Nonetheless, even assuming that there might have been some legal content on the [redacted] website, as the Fourth Circuit has made clear, is it not necessary for an affidavit to "'rule out a suspect's innocent explanation for suspicious facts' to obtain a warrant.'"

[8] According to the Affidavit, "hurtcore" refers to violent pornography. Affidavit ¶ 17.

Bosyk, 933 F.3d at 325 (quoting *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018)). Rather, the Affidavit need only set forth facts—which it does here—to show a fair probability that child sexual abuse and exploitation material would be found at the residence of the user of the Target IP Address. *See id.* at 327-28.

III.

Next, the defendant argues that, even if the Magistrate Judge had a substantial basis for finding probable cause to issue a search warrant, that finding relied on intentionally or recklessly false statements or omissions by Special Agent Ford in the Affidavit. Specifically, defendant argues that he is entitled to an evidentiary hearing and the suppression of all evidence derived from the allegedly illegal search of his home pursuant to *Franks v. Delaware*. 438 U.S. 154 (1978). This argument fails, as a careful reading of the Affidavit discloses that Special Agent Ford's statements or omissions were neither false nor misleading.

In *Franks v. Delaware*, the Supreme Court set out the "limited circumstances in which a defendant can attack a facially sufficient warrant affidavit" and obtain an evidentiary hearing to challenge the warrant. *United States v. Clenney*, 631 F.3d 658, 663 (4th Cir. 2011) (citing *Franks*, 438 U.S. at 155-56). As *Franks* teaches, in order to obtain an evidentiary hearing, the defendant must make a "substantial preliminary showing" that the affiant made "a false statement knowingly and intentionally, or with reckless disregard for the truth" that is "necessary to the finding of probable cause." *Franks*, 438 U.S. at 155–56. In order to succeed on a motion for a *Franks* hearing based on omissions, the defendant must show that the omissions were "'designed to mislead, or . . . made in reckless disregard of whether they would mislead' and that the omissions were material, meaning that their 'inclusion in the affidavit would defeat probable cause.'" *Clenney*, 631 F.3d at 664 (emphasis omitted) (quoting *United States v. Colkley*, 899

F.2d 297, 301 (4th Cir. 1990)). The defendant has failed to make a substantial preliminary showing that Special Agent Ford made material statements or omissions that were false or misleading and thus is not entitled to a *Franks* hearing.

In his Motions to Suppress, defendant argues that Special Agent Ford made material false statements or omissions in the Affidavit regarding (1) Paragraph 23 of the Affidavit, (2) Paragraph 25 of the Affidavit, and (3) various other parts of the Affidavit, including portions discussing (i) Tor, (ii) the [redacted] website, (iii) the locations where forensic evidence could be found, and (iv) the defendant's residence. The defendant's arguments are unconvincing.

In its entirety, Paragraph 23 of the Affidavit states:

> In August 2019, a foreign law enforcement agency ("FLA") known to the FBI and with a history of providing reliable, accurate information in the past, notified the FBI that the FLA determined that on May 23, 2019, a user of the [Target IP address] accessed online child sexual abuse and exploitation material via a website that the FLA named and described as the TARGET WEBSITE.

Affidavit ¶ 23.

Contrary to defendant's argument, Paragraph 23 contains no material misrepresentations or omissions, intentional or otherwise. Rather, the paragraph simply repeats, essentially verbatim, the tip [redacted]: The FLA Tip reported that the defendant's IP address "was used to access online child sexual abuse and exploitation material." FLA Tip. Paragraph 23 repeats the tip almost verbatim, stating that the IP address "accessed online child sexual abuse and exploitation material." Affidavit ¶ 23.[9] Because Paragraph 23 accurately and clearly conveys the FLA Tip, it is not intentionally or recklessly misleading in any respect.

[9] Nor does defendant rescue his argument by noting the addition of "via a website" in Paragraph 23. The addition of "via a website" is not misleading both because an internet user cannot access any material online without accessing a website and because the addition connects the information relayed in the FLA Tip with the name of the website derived from the FLA [redacted] Report.

It is clear from defendant's Motion that his primary concern with Paragraph 23 is that the use of the tip's phrase that the IP address "accessed online child sexual abuse and exploitation material" invites the inference that defendant *viewed* child abuse and exploitation material when, as the defendant sees it, the evidence shows no more than that defendant briefly visited the website.[10] As noted previously, the fact that the FLA informed the FBI that defendant's IP address accessed the Tor hidden service [redacted] clearly invites and warrants the reasonable inference that the IP address user was purposeful in his efforts to reach the [redacted] website and its illegal content. This inference follows from the fact—as the Affidavit makes clear—that in order to navigate to the [redacted] website, an internet user had to follow certain specific steps, including downloading the Tor browser, finding a directory or search website with a link to the [redacted] website, and finally navigating to the [redacted] website itself. Given the involved set of steps necessary to access the Tor hidden service [redacted], the Magistrate Judge clearly had a substantial basis to conclude that there was a fair probability of finding contraband—child pornography—at the target residence. Thus, with respect to Paragraph 23, defendant's argument falls far short of making the requisite preliminary showing that anything in Paragraph 23 was false or misleading. The defendant is therefore not entitled to a *Franks* hearing in this respect.

Defendant's arguments relating to Paragraph 25 are similarly unavailing. Defendant claims that Special Agent Ford made material false statements or omissions in Paragraph 25 of the Affidavit, which, in its pertinent parts, states:

> The FLA . . . advised U.S. law enforcement that the FLA had not interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain that IP address information.

---

[10] Defendant suggests that the timestamp in the FLA Tip that specified the time, down to the second, that the Target IP Address user accessed child abuse and exploitation material meant that the defendant had only accessed the [redacted] website for that single second. This is an unwarranted conclusion. Far more likely is the inference that the timestamp refers only to the time the Target IP Address user arrived at the [redacted] website, not how much time was spent viewing child sexual abuse and exploitation material on the [redacted] website.

Affidavit ¶ 25; *see also* FLA Letter.

Here again, Special Agent Ford merely reported what the FLA Letter stated. *See* FLA Letter. Defendant speculates that the FLA must have used a technique that interferes with a computer in the United States in order to obtain defendant's IP address and therefore that the FLA's—and the Affidavit's—statement to the contrary is false. This claim is rank speculation, as is defendant's contention that Special Agent Ford knew—or should have known—that the FLA must have interfered with a computer in the United States. None of defendant's experts in their declarations establish that the FLA could not have obtained defendant's IP address without interfering with a computer in the United States. At most, defendant's experts say that, in their opinion, it is "most likely" that the FLA had to interfere with a computer in the United States in order to identify defendant's IP address.[11] Beyond defendant's questionable interpretation of his own experts' declarations, defendant offers no evidence in support of his contention that the FLA interfered with his computer and that Special Agent Ford knew as much. There is no persuasive reason to doubt the veracity of the FLA's statement that it did not interfere with a computer in the United States, nor is there any persuasive reason to think that Special Agent Ford should have disbelieved the FLA's statement. Defendant's speculation to the contrary does not amount

[11] *See* Third Declaration of Dr. Matthew Miller, Def. Mem. in Sup. of Mot. to Suppress No. 4, Ex. 5, at 1-2 (stating that "the [FLA] most likely had to interfere with the Tor Browser's security protections to take control of, access, interfere with and/or search" defendant's computer); Declaration of Richard Clayton, Def. Mem. in Sup. of Mot. to Suppress No. 4, Ex. 9, at 10 ("I consider it most likely that in this case an active attack was used to identify a visitor to the Tor hidden service."). Special Agent Ford provided a declaration contradicting defendant's assertion and presenting possible publicly known methods of de-anonymizing Tor users without interfering with the user's computer. Declaration of Special Agent Christopher Ford, Gov't Suppl. Br. in Opp. to Def. Mot. to Compel, Ex. 2. Defendant's experts disputed whether the methods proposed by Special Agent Ford were practically possible and maintained that it was most likely that the FLA had interfered with defendant's computer. *See* Third Declaration of Dr. Matthew Miller, at 1-2 (arguing that the alternative method put forward by Special Agent Ford was "extremely unlikely" to have been used).

to the substantial preliminary showing required by *Franks*.[12] In sum, defendant's argument with respect to Paragraph 25 falls well short of demonstrating, as required by *Franks*, that Special Agent Ford intentionally or recklessly made a materially false statement in his Affidavit.

Defendant further moves to suppress the evidence obtained from the search based on allegedly materially misleading statements and omissions in the Affidavit regarding (i) Tor, (ii) the [redacted] website, (iii) the locations where forensic evidence could be found, and (iv) the target residence. Defendant's arguments are unsuccessful.

Defendant first argues that the Affidavit fails to provide a complete characterization of Tor and inappropriately attaches suspicion to defendant's use of Tor. *See* Def. Mem. in Sup. of Mot. to Suppress No. 3, at 17. Yet, the defendant fails to identify any false statements in the Affidavit and fails to show that any omissions were either material or "designed to mislead, or . . . made in reckless disregard of whether they would mislead." *Colkley,* 899 F.2d at 301. The Affidavit provides an accurate description of Tor as well as the steps necessary for an internet user to access a Tor hidden service such as the [redacted] website. Furthermore, as the Fourth Circuit has emphasized, "agents need not include disclaimers specifically pointing out facts absent from the affidavit to obtain a warrant." *Bosyk*, 933 F.3d at 332. Rather, "[a] warrant application is 'judged on the adequacy of what it does contain, not on what it lacks, or on what a critic might say should have been added.'" *Id.* (quoting *United States v. Allen*, 211 F.3d 970, 975

[12] The government incorrectly states that the defendant must show that "it would be impossible for the FLA to have obtained the Target IP in a manner consistent with what the tip states." Gov. Omnibus Resp. to Def. Mot. to Suppress, at 20-21, Dkt. 101. The defendant need not necessarily prove that it would be *impossible*. Rather, the defendant must make a substantial preliminary showing that the affiant made "a false statement knowingly and intentionally, or with reckless disregard for the truth" that is "necessary to the finding of probable cause." *Franks*, 438 U.S. at 155–56. Defendant has failed to do so.

(6th Cir. 2000) (en banc)). Here, Special Agent Ford accurately describes Tor and does not misleadingly omit any material information.[13]

Defendant next argues that the Affidavit misled the Magistrate Judge about the [redacted] website. The defendant claims that the Affidavit inaccurately describes the [redacted] website as being "dedicated to the advertisement and distribution of child pornography," when in reality the site did not advertise child pornography and contained both legal and illegal content. Def. Mem. in Sup. of Mot. to Suppress No. 3, at 18 (quoting Affidavit ¶ 15). The defendant claims that the Affidavit incorrectly describes the [redacted] website because the site contains both legal and illegal content. This is not so.

The Affidavit clearly describes the [redacted] website—including that the site was created to host content featuring "18 (twinks) and younger," the detail that defendant claims precludes a finding of probable cause. Affidavit ¶ 17. Defendant's claim that the site included legal content—citing "18" and "hurtcore" content—does not make it so. As described above, that claim is contradicted by screenshots of the site provided by the FBI, which display the [redacted] website's board index divided into categories for "Ages 0-5," "Ages 6-13," and "Ages 14+". [redacted] Board Index, Def. Ex. 10, Dkt 86. Even the subforum for "Regular Porn" has a subheading of "[t]eens and under." *Id.* Thus, Special Agent Ford's description of the [redacted] website is accurate and without any materially misleading omissions.

Defendant next contends that the Affidavit contained misleading statements regarding the locations where forensic evidence could be found. Defendant cites his expert, Dr. Matthew

[13] On October 26, 2020, defendant supplied supplemental authority for his assertions regarding Tor, arguing that the government's Complaint in *United States v. Google* provides support for his contention that people commonly download non-default browsers and that people may download the Tor browser due to privacy concerns. *United States v. Google*, 1:20-cv-3010, Complaint, October 20, 2020, Dkt 1. Defendant's supplemental briefing fails to provide any persuasive rationale to find Special Agent Ford's accurate statements regarding Tor to be false or misleading. Nor is the omission of further information regarding Tor "designed to mislead, or . . . made in reckless disregard of whether they would mislead." *Colkley*, 899 F.2d at 301. Defendant is therefore not entitled to a *Franks* hearing in this regard.

Miller, to argue that because the Tor browser does not save traces or footprints of the internet user's activity, investigators would not be able to find traces or footprints saved to the IP Address user's computer eight months later. Fourth Declaration of Dr. Matthew Miller, Ex. 6, at 7, Dkt. 84.[14] Even assuming that Paragraph 36(h) reflects a misunderstanding of how Tor works, this paragraph is not necessary for the Magistrate Judge's finding of probable cause. The Affidavit accurately describes the characteristics common to individuals with a sexual interest in children as including the storage of child pornography for long periods of time on digital devices. Affidavit ¶¶ 41-42; *see also Bosyk*, 933 F.3d at 331. The Affidavit further describes the difficulty of accessing Tor hidden services, reflecting the likelihood that the internet user would store information relating to the [redacted] website or a directory site in order to navigate to the site. Affidavit ¶ 27. Thus, Paragraph 36(h), though possibly reflecting a misunderstanding of how the Tor browser works, is not necessary for the finding of probable cause. The defendant is therefore not entitled to a *Franks* hearing on this basis.

Finally, defendant argues that the Affidavit made materially misleading omissions regarding the target residence, as it omitted noting that Risa Sanders, the defendant's mother and one of the residents of the subject premises, is a licensed clinical psychologist. This argument is completely unpersuasive. Accessing child sexual abuse and exploitation material violates the law regardless of whether it is Risa Sanders or the defendant using the computer. This omission is neither misleading nor material. Therefore, defendant is not entitled to a *Franks* hearing.

[14] The Affidavit points out that internet users seeking to access Tor hidden services can install the Tor Browser or manually configure a web browser to access the Tor network. Affidavit ¶ 9 n.2. The latter method, which defendant's experts do not address, could potentially create a cache, thus leaving the traces or "footprints" that could be found months later as described in the Affidavit. However, given that the Affidavit relegates this possibility to a short footnote and does not reference it in later summaries in support of finding probable cause, that possibility will not be considered in determining whether the Affidavit's misstatement regarding Tor in Paragraph 36(h) is material.

In summary, defendant is not entitled to a *Franks* hearing because defendant failed to make a substantial preliminary showing that Special Agent Ford made a false statement knowingly and intentionally, or with reckless disregard for the truth that is necessary to find probable cause. Defendant is also not entitled to suppression because the Magistrate Judge had a substantial basis for determining the existence of probable cause and because defendant failed to show that a Fourth Amendment violation occurred.[15] Defendant's Motions to Suppress therefore must be denied.

Finally, it appears that it is not necessary for this Memorandum Opinion to be sealed. As such, the Memorandum Opinion will be unsealed in three days unless a motion is filed beforehand establishing good cause to keep the Memorandum Opinion under seal.

An appropriate Order will issue separately.

The Clerk is directed to send a copy of this Sealed Memorandum Opinion to all counsel of record.

Alexandria, Virginia
October 26, 2020

/s/
T. S. Ellis, III
United States District Judge

[15] Although it is not necessary to reach or decide whether the *Leon* good faith exception applies here because the search was legal, there is little doubt that *Leon* would rescue the search because none of the exceptions noted in *Leon* apply. *United States v. Leon*, 468 U.S. 897, 920 (1984); *see also United States v. Doyle*, 650 F.3d 460, 467 (4th Cir. 2011).